2N PICard Commander

Uživatelský manuál

2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Obsah

Použité symboly a termíny

V manuálu jsou použity následující symboly a piktogramy:

NEBEZPEČÍ
Vždy dodržujte tyto pokyny, abyste se vyhnuli nebezpečí úrazu.

VAROVÁNÍ
Vždy dodržujte tyto pokyny, abyste se vyvarovali poškození zařízení.

VÝSTRAHA
Důležité upozornění. Nedodržení pokynů může vést k nesprávné funkci zařízení.

TIP
Užitečné informace pro snazší a rychlejší používání nebo nastavení.

POZNÁMKA
Postupy a rady pro efektivní využití vlastností zařízení.

Popis produktu

PICard Commander je softwarová aplikace pro šifrování přihlašovacích údajů na přístupových kartách. Aplikace vytváří projekty, které vygenerují sadu šifrovacích a čtecích klíčů. Čtecí klíče projektu lze importovat do 2N zařízení nebo do Access Commanderu, který následně zajišťuje distribuci čtecích klíčů do připojených 2N zařízení.

Technologie 2N PICard je určena pro šifrování karet MIFARE® DESFire® EV2 a MIFARE® DESFire® EV3.

V aplikaci PICard Commander je možné nahraná data na přístupových kartách mazat.

Funkce aplikace PICard Commander je podmíněna zakoupením licence.

Související produkty

Objednací číslo: 91379601

2N PICard Commander Licence

Licence je vydávána vždy pro konkrétní USB čtečku karet na základě Device key dané čtečky. Device key čtečky lze před nahráním licence zjistit v PICard Commander. Podporované USB čtečky karet jsou uvedeny níže.

Objednací číslo: 9137421E

USB čtečka 13.56 MHz, 125 kHz RFID karet a NFC/HCE zařízení

Externí čtečka RFID karet pro připojení k PC pomocí USB rozhraní. Vhodná pro správu systému a přidávání 13.56 MHz, 125 kHz karet a Android zařízení s podporou NFC/HCE pomocí webového rozhraní 2N IP interkomu nebo aplikace Access Commander. Vhodná pro nahrání MIFARE DESFire karet do šifrovací aplikace PICard Commander[a]. Čte stejné typy karet a zařízení jako čtečky karet v 2N IP interkomech:

Podporované RFID karty 125 kHZ:

- EM4x02
- NXP HiTag2

Podporované RFID karty 13.56 MHz:

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **Mobile Key**

Objednací číslo: 9137424E

Zabezpečená USB čtečka 13.56 MHz, 125 kHz RFID karet a NFC/HCE zařízení

Externí zabezpečená čtečka RFID karet pro připojení k PC pomocí USB rozhraní. Vhodná pro správu systému a přidávání 13.56 MHz, 125 kHz karet a Android zařízení s podporou NFC/HCE pomocí webového rozhraní 2N IP interkomu nebo aplikace Access Commander. Vhodná pro nahrání MIFARE DESFire karet do šifrovací aplikace 2N PICard Commander[a]. Čte stejné typy karet a zařízení jako čtečky karet ve 2N IP interkomech:

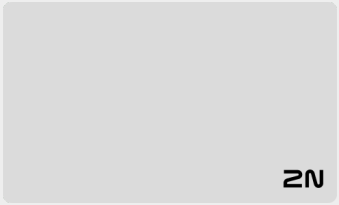
125 kHz

- EM4xxx
- HID Prox

13.56 MHz

- ISO14443A (MIFARE DESFire)
- PicoPass (HID iClass)
- FeliCa
- ST SR(IX)

- 2N Mobile Key
- HID SE (Seos, iClass SE, MIFARE SE)



Objednací číslo: 11202601

2N RFID karta MIFARE Desfire EV3 4K 13.56MH 10 ks

balení 10 ks

MIFARE DESFire EV3 (ISO14443A)

Objednací číslo: 11202602

2N RFID fob MIFARE Desfire EV3 4K 13.56MHz 10 ks

balení 10 ks

MIFARE DESFire EV3 (ISO14443A)

[a] Technologie 2N PICard je určena pro šifrování karet MIFARE DESFireEV2 a MIFARE DESFire EV3.

Kompatibilní zařízení

Karty s technologií PICard lze číst na následujících zařízení:

2N IP Style

- 2N IP Style main unit
  (obj. č. 9157101)
- 2N IP Style main unit, secured
  (obj. č. 9157101-S)

2N IP Verso

- 2N IP Verso – 13.56MHz secured card reader, NFC, reads UID + PACS ID
  (obj. č. 9155086/9155042)
- 2N IP Verso Bluetooth & RFID reader 125kHz, 13.56MHz, NFC
  (obj. č. 91550945)
- 2N IP Verso Bluetooth & RFID reader 125kHz, secured 13.56MHz, NFC
  (obj. č. 91550945-S
- 2N IP Verso Touch keypad & RFID reader 125kHz, 13.56MHz, NFC
  (obj. č. 91550946)
- 2N IP Verso Touch keypad & RFID reader 125kHz, secured 13.56MHz, NFC
  (obj. č. 91550946-S)

2N Access Unit

- 2N Access Unit 2.0 13.56 MHz, NFC
  (obj. č. 9160342)
- 2N Access Unit 2.0 secured 13.56 MHz, NFC
  (obj. č. 9160342-S)
- 2N Access Unit 2.0 125kHz, 13.56MHz, NFC
  (obj. č. 9160344)
- 2N Access Unit 2.0 125kHz, secured 13.56MHz, NFC
  (obj. č. 9160344-S)
- 2N Access Unit 2.0 Bluetooth & RFID – 125kHz, 13.56MHz, NFC
  (obj. č. 9160345)
- 2N Access Unit 2.0 Bluetooth & RFID – 125kHz, secured 13.56MHz, NFC
  (obj. č. 9160345-S)

- 2N Access Unit 2.0 Touch keypad & RFID – 125kHz, 13.56MHz, NFC
  (obj. č. 9160346)
- 2N Access Unit 2.0 Touch keypad & RFID – 125kHz, secured 13.56MHz, NFC
  (obj. č. 9160346-S)

2N Access unit M

- 2N Access Unit M 13.56 MHz, NFC ready
  (obj. č. 916112)
- 2N Access Unit M RFID – 125kHz, 13.56MHz, NFC
  (obj. č. 916114)
- 2N Access Unit M Bluetooth & RFID – 125kHz, 13.56MHz, NFC
  (obj. č. 916115)
- 2N Access Unit M Touch keypad & RFID – 125kHz, 13.56MHz, NFC
  (obj. č. 916116)

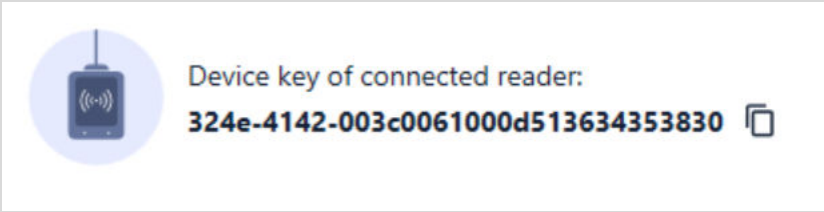
2N IP Force

- 2N IP Force 13.56MHz card reader, NFC ready, reads UID
  (obj. č. 9151031)
- 2N IP Force 13.56MHz card reader, NFC ready, reads UID + PACS ID
  (obj. č. 9151031S)

Instalace a načtení licence

1. Nainstalujte PICard Commander běžným způsobem přes instalační program.
2. Po spuštění aplikace nahrajte licenci kliknutím na Load License v oranžové liště (nebo v záložce Help → License). Následně načtěte licenční soubor z disku. Pro úspěšné nahrání licence musí být čtečka karet připojena k počítači.

POZNÁMKA
Licence je vázána na konkrétní USB čtečku karet. K získání licence je proto nutné uvést Device key zařízení čtečky, který se nachází v informacích o licenci v PICard Commanderu (záložka Help > License). Pro zobrazení klíče musí být čtečka karet připojena k počítači.



Připojení jiné čtečky

Pokud je k počítači připojena jiná čtečka než ta, která je spárovaná s používanou licencí, aplikace PICard Commander na to po spuštění upozorní. V záložce Help > License lze nahrát novou licenci.

Projekt

Zakládání jednotlivých projektů umožňuje šifrovat skupiny přístupových karet v různých módech. Každý projekt můžete nastavit specificky pro daný účel použití karet. Projekt generuje sérii šifrovacích a čtecích klíčů. Do zařízení nebo do Access Commanderu lze nahrát čtecí klíče vždy jen jednoho projektu.

Založení nového projektu

Po otevření aplikace založte nový projekt stisknutím tlačítka **Start new project**.

Alternativní cesta: záložka *File* > *New project*

Otevře se průvodce nastavením nového projektu, dále postupujte podle Nastavení projektu [9].

Otevření projektu

1. V úvodním rozhraní aplikace klikněte na tlačítko Open project.
   Alternativní cesta: záložka *File* > *Open project*

Naposledy otevřené projekty se zobrazují ve spodní sekci úvodního rozhraní aplikace.

Nastavení projektu

Při zakládání projektu je nutné nastavit jeho parametry.

Nastavení lze později změnit v Project configuration v úvodním rozhraní aplikace (alternativní cesta: záložka Project > Change configuration).

Základní údaje (Basic settings)

- **Project name** – název projektu
- **Project description** – prostor pro vepsání poznámek k projektu

Hlavní šifrovací klíč (Main Encryption Key)

Podle hlavního šifrovací klíč (MEK) generuje aplikace PICard Commander sadu klíčů k zašifrování přístupových údajů karet. Klíč by tak měl být unikátní a dostatečně bezpečný. Sada klíčů vychází z hlavního šifrovacího klíče, proto projekty se stejným hlavním šifrovacím klíčem generují stejné sady klíčů. Při ztrátě projektu je možné vytvořit nový projekt se stejným hlavním šifrovacím klíčem a pokračovat s šifrováním dalších karet. Čtecí klíče ztraceného projektu, které již byly nahrané do 2N zařízení, budou platné i pro nově zašifrované karty.

VAROVÁNÍ
Hlavní šifrovací klíč nelze později **zobrazit ani změnit**.

TIP
Pro maximální bezpečnost je důležité uschovat jak samotný soubor s projektem, tak hlavní šifrovací klíč (MEK). Ideální je si hlavní šifrovací klíč (MEK) bezpečně uložit mimo online prostředí, např. do trezoru, bezpečnostní schránky apod.

Mód šifrování (Card mode)

Je možné volit z následujících módů šifrování karet:

- **Card may be used for other applications later on (best compatibility)** – Karty budou využívány především systémy 2N. Data na kartě budou zašifrována, ale jejich UID zůstane čitelné pro aplikace třetích stran. Karty je možné přeformátovat do původního stavu.
- **Card will be used only for access control with 2N devices (best privacy)** – Karty budou využívány výhradně v systémech 2N. Dojde k trvalému přenastavení parametrů karty. Při zašifrování se na kartě aktivuje funkce Random ID.
- **Card is already used for other applications (advance settings)** – Na kartách již jsou nahrané aplikace třetích stran. V dalším kroku lze nastavit vybrané parametry karet MIFARE DESFire, jejichž přístupové údaje má technologie 2N PICard v projektu šifrovat.

POZNÁMKA
Výběr módu **Card is already used for other applications** je nevratný.

V dalším kroku lze vyplnit:

- **Application ID (AID)** – kód, pod kterým bude aplikace 2N PICard na kartě identifikována. AID je přednastaveno na 53324E.
- **PICC master key type** – typ PICC master key nastaveného na kartách, které má aplikace 2N Picard šifrovat.
- **PICC master key** – hodnota PICC master key karet, které má aplikace 2N Picard šifrovat.
- **Enable randomisation of readable card ID** – zapnutí funkce Random ID zajistí, že se UID karty při každém jejím načtení náhodně změní. Neautorizovaná osoba tedy nemůže kartu zneužít k identifikaci jejího držitele.
- **Encrypt cards in factory default state (change default PICC master key)** – možnost volby nahrát zadaný PICC master key na další prázdné karty při jejich šifrování v projektu. Není-li tato možnost vybrána, PICard Commander prázdnou kartu odmítne šifrovat.

VAROVÁNÍ

- Po procesu šifrování karet pod novým AID je třeba znovu exportovat čtecí klíče. Dříve zašifrované karty se starým AID se stanou pro 2N zařízení nečitelné.
- Změnou PICC master key v projektu s již zašifrovanými kartami dojde ke znemožnění tyto karty dále v projektu upravovat a mazat jejich data. Na platnost karet pro autentizaci ve 2N zařízení nebude mít změna vliv.
- Zapnutí funkce Random ID karty je nevratné. Původní UID karty zůstane nečitelné i po formátování karty.

Uložení na disku

Soubor projektu se uloží na disku jako *Nazevprojektu*.picprj.

Zaškrtnutí políčka **Protect project file with password** umožní nastavit ochranné heslo pro otevření projektu. Heslo je možné později změnit v záložce Project > Change protection password.

VAROVÁNÍ
Zapomenuté heslo nelze později **zobrazit ani obnovit**.

Šifrování a čtení karet

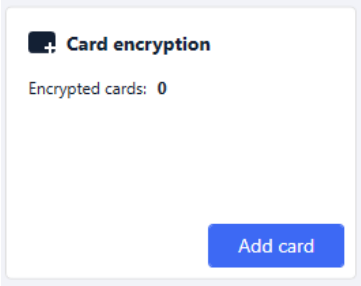
Zde je přehled toho, co v kapitole naleznete:

Šifrování karet

Proces šifrování karet ve PICard Commander přidělí každé kartě unikátní 128bitový identifikátor, který je následně zašifrován pomocí šifrovacích klíčů příslušného projektu. V projektu je možné kartu načíst a zjistit tak její přidělený identifikátor, případně další informace o kartě a zda je možné ji v projektu šifrovat.

Proces šifrování

1. V úvodním rozhraní aplikace klikněte na **Add card** v sekci **Card encryption**.
   Alternativní cesta: záložka *Project* > *Encrypt New Card*



   Credential ID for new card – nový identifikátor nahrávané karty
2. Položte kartu na čtečku. Stisknutím tlačítka **Encrypt** se kartě přiřadí přístupové údaje, které se současně se zašifrují.

> **TIP**
> Zaškrtnutím políčka vpravo můžete spustit automatické šifrování dalších přiložených karet bez nutnosti opakovaného stisknutí tlačítka **Encrypt**.

Aplikace informuje o úspěšném zašifrování karty.

Pokud se kartu nepodařilo zašifrovat, aplikace informuje o důvodu:

- **Card cannot be encrypted** – aplikace PICard Commander nemá přístup k PICC master key karty. Pokud chcete šifrovat karty s přednastaveným PICC master key, je potřeba vybrat příslušný mód šifrování v Nastavení projektu [9].
- **Not enough free space on card** – na kartě není dostatek místa pro nahrání technologie 2N PICard. Minimální požadovaná paměť je 512 B.
- **Unsupported card** – aplikace tento typ karty nepodporuje. Technologie 2N PICard je určena k šifrování karet MIFARE DESFire EV2 a EV3.
- **Only MIFARE DESFire EV2 or EV3 are supported** – aplikace tento typ karty nepodporuje. Načtená karta je MIFARE DESFire EV1.
- **Communication failure with card** – čtečce se nepodařilo kartu načíst. Přiložte kartu ke čtečce a neoddalujte ji před ukončením procesu šifrování.

TIP
Ve spodní sekci okna se nachází rozbalovací seznam identifikátorů šifrovaných karet. Pokud chcete seznam evidovat, zkopírujte jej před zavřením okna. Zavřením okna se seznam smaže. Později lze zobrazit identifikátory jen pro jednotlivé karty.

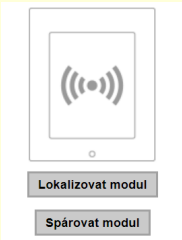
Export čtecích klíčů

Aby mohla mít zařízení 2N přístup k datům na zašifrovaných kartách, potřebují znát čtecí klíče daného projektu. Z aplikace PICard Commander lze čtecí klíče exportovat do 2N zařízení nebo do Access Commanderu, který zajišťuje distribuci do všech připojených zařízení 2N. Jakmile jsou do zařízení čtecí klíče nahrány, budou zařízení schopna číst i karty, které byly v daném projektu zašifrovány až po nahrání čtecích klíčů.

1. V úvodním rozhraní aplikace klikněte na Export v sekci Reader keys export (alternativní cesta: záložka Project > Export reader keys).
2. Čtecí klíče projektu můžete exportovat dvěma způsoby:

   - Export keys to file [13]
   - Upload keys to Access Commander [14]

VÝSTRAHA
Pokud k zařízení 2N, ve kterém jsou nahrané čtecí klíče, nově připojíte rozšiřující modul čtečky RFID karet pomocí VBUS kabelu, je potřeba tento modul se zařízením spárovat. Spárování rozšiřujícího modulu čtečky provedete přes webové rozhraní zařízení v sekci Hardware, v menu Rozšiřující moduly.

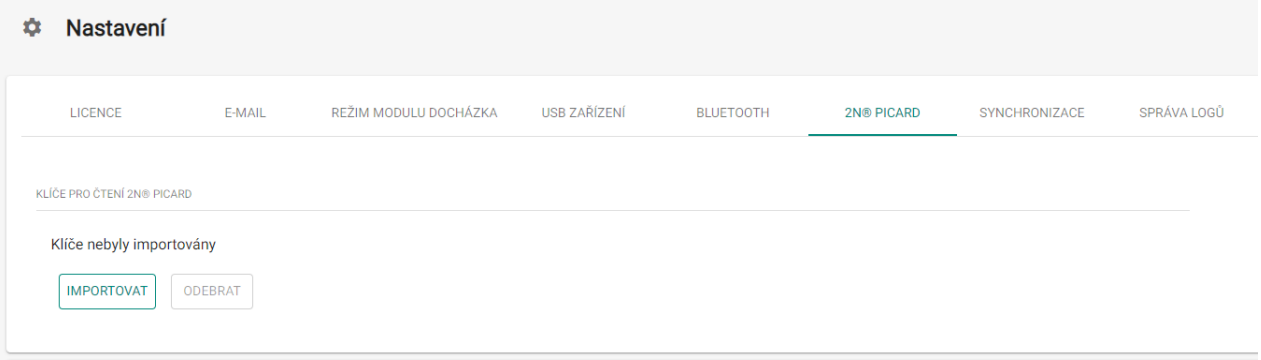


Export keys to file

Aplikace vygeneruje soubor s klíči a uloží jej na disk. Soubor je následně potřeba importovat do nastavení zařízení 2N nebo do Access Commanderu přes jejich webová rozhraní. V dalším kroku exportu je možné nastavit ochranné heslo ukládaného souboru.

- **Import do Access Commanderu (verze 3.00 a vyšší)** přes webové rozhraní: Nastavení > Přístupy > karta PICard klíče > Importovat

- **Import do Access Commanderu** přes webové rozhraní: sekce Nastavení systému > 2N PICARD > IMPORTOVAT



- **Import do 2N zařízení** přes webové rozhraní: sekce Služby > menu Řízení přístupu > záložka PICard > 

Upload keys to Access Commander

Aplikace PICard Commander nahraje čtecí klíče přímo do Access Commanderu, který zajistí následnou distribuci do připojených zařízení 2N. V dalším kroku je nutné zadat administrátorské přihlašovací údaje k licenci Access Commanderu.

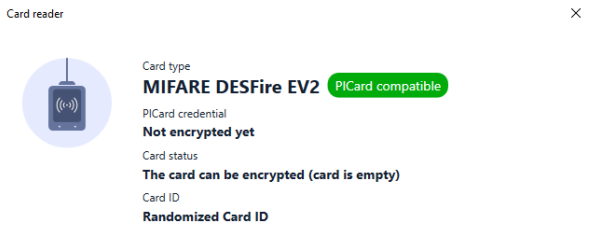
Address – HTTP adresa webového rozhraní Access Commanderu

Login name – přihlašovací jméno administrátorského účtu v Access Commanderu

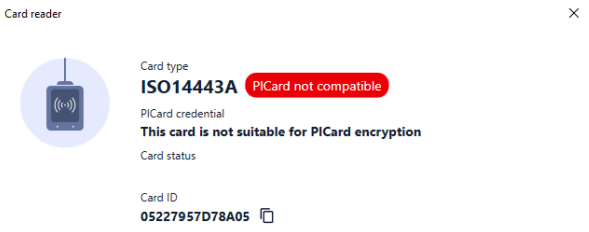
Password– přihlašovací heslo k danému účtu v Access Commanderu

Čtení informací o kartě

Přidělený identifikátor karty a další informace o kartě a o jejích možnostech šifrování je možné zobrazit v záložce *Project* > *Read card.* Informace se načtou po přiložení karty ke čtečce.



Tuto kartu lze v aplikaci šifrovat.



Kartu tohoto typu nelze v aplikaci šifrovat.

PICard credential načte identifikátor karty přidělený při procesu šifrování. Pokud karta identifikátor nemá, objeví se informace o možnostech jeho přidělení:

- **Not encryptable** – typ karty je kompatibilní s technologií 2N PICard, ale projekt nemá přístup k jejímu PICC master key.
- **This card is not suitable for PICard encryption** – aplikace tento typ karty nepodporuje. Technologie 2N PICard je určena pro šifrování karet MIFARE DESFire EV2 a EV3.
- **Not encrypted yet** – kartu je možné šifrovat.
- **Unknown** – karta je zašifrovaná v jiném projektu pod odlišným hlavním šifrovacím klíčem. Karta může být také poškozena.

Card Status zobrazí stav nebo možnosti zašifrování dané karty:

- **Valid PICard credential** – karta je v zašifrovaná v tomto projektu.

- **The card can be encrypted (card is empty)** – karta není zašifrovaná. Na kartě je tovární nastavení.
- **The card can be encrypted** – karta není zašifrovaná. Na kartě je nastaven PICC master key kompatibilní s tímto projektem.
- **Different PICC Master Key detected. Card's current PICC Master Key required for encryption** – kartu nelze v tomto projektu zašifrovat. Nastavený PICC master key se liší.
- **PICard application created in a different project, so cannot be read in this project** – karta je zašifrovaná v jiném projektu.
- **Only MIFARE DESFire EV2 or EV3 are supported** – kartu nelze zašifrovat. Aplikace tento typ karty nepodporuje. Načtená karta je MIFARE DESFire EV1.
- **INVALID CREDENTIAL (there's a problem with the digital signature)** – zašifrované přístupové údaje karty nelze zobrazit. Potvrzení jejich autenticity se nezdařilo. Digitální podpis je neplatný.

Card ID zobrazí UUID karty nebo informuje o zapnuté funkci Random ID.

Mazání dat na kartě

Aplikace PICard Commander umožňuje formátovat karty nebo vymazat jejich zašifrované přístupové údaje. Karty je možné mazat a formátovat pouze v projektu, ve kterém jsou zašifrovány.

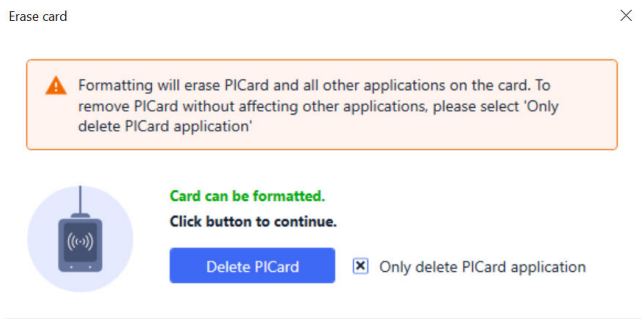
Formátování karty

VAROVÁNÍ
Při formátování karty se smažou veškerá data na kartě včetně dat třetích stran.

1. Otevřete záložku Project > Format card. Přiložte kartu ke čtečce. Stisknutím tlačítka Format card se karta naformátuje.

POZNÁMKA
Pokud je na kartě zapnuta funkce Random ID, formátování karty čitelnost původního UID neobnoví.

Smazání přístupových údajů



1. Otevřete záložku Project > Format Card.
2. Zaškrtněte políčko **Only delete PICard application**.
3. Přiložte kartu ke čtečce.
4. Stisknutím tlačítka Delete PICard se vymažou zašifrované přístupové údaje karty.

Licence třetích stran

Kompletní seznam použitých licencí knihoven třetích stran je uveden v záložce Help > About.

wiki.2n.com

2N PICard Commander – Uživatelský manuál

2N.com